Deutscher Bundestag **Drucksache 19/10336**
19. Wahlperiode 17.05.2019

Antwort
der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Heike Hänsel, Andrej Hunko, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/9592 –

Fähigkeiten der „Cyber-Truppe“ der Bundeswehr

Vorbemerkung der Fragesteller

Der „Cyber-Raum“ gehört in den letzten Jahren zu den heißen Themen der Militärberichterstattung (http://augengeradeaus.net/2018/10/cyber-cyber-die-meldungen-nur-eines-tages/#more-31555).

Dabei bleibt nicht nur die Gewinnung geeigneter IT-Kräfte schwierig und die Definition der Einsatzspektren vage. Wie beim Einsatz militärischer IT-Kräfte das Völkerrecht eingehalten werden kann, z. B. was die verlässliche Attribution von Angriffen und die klare Unterscheidung ziviler und militärischer Angriffsziele angeht, ist noch nicht erkennbar. Bis jetzt fehlt es außerdem an einer nachvollziehbaren Darstellung, inwieweit die Bundesregierung gewährleisten kann, dass bei einem Einsatz ihrer „Cyber-Krieger“ der verfassungsrechtliche Parlamentsvorbehalt nicht verletzt wird – und das nicht nur dann, wenn es darum geht, bereits vor einem Bundeswehreinsatz fremde Netze zu infiltrieren. In keinem Mandatsantrag der Bundesregierung fand bislang der Einsatz von IT-Kräften bei Bundeswehreinsätzen auch nur Erwähnung.

Vorbemerkung der Bundesregierung

Die parlamentarische Kontrolle der Bundeswehr erfolgt im Rechtsrahmen, der durch das Grundgesetz gesteckt wird. Dies betrifft die militärischen Fähigkeiten in der Dimension Cyber- und Informationsraum in gleicher Weise wie die anderen militärischen Fähigkeiten der Bundeswehr. Somit unterliegen die Cyber-Fähigkeiten der Bundeswehr derselben parlamentarischen Kontrolle wie andere militärische Fähigkeiten.

Die Beantwortung der Fragen erfolgt in dem Verständnis, dass die Fragesteller mit „IT-Kräften“ die Teile der Streitkräfte bezeichnen, die im militärischen Organisationsbereich Cyber- und Informationsraum (OrgBerCIR) gebündelt sind, um zur Erzeugung eines gemeinsamen Lagebildes, zum Schutz des eigenen IT-Systems und zur Wirkung in der Dimension CIR beizutragen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 14. Mai 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Darüber hinaus wird darauf hingewiesen, dass in Mandatsanträgen nicht von einzelnen Kräftedispositiven, sondern von militärischen Fähigkeiten (bspw. zur Aufklärung oder zur Führungsunterstützung) die Rede ist. Deshalb können selbstverständlich regelmäßig auch Kräfte des OrgBerCIR im Rahmen der mandatierten Einsätze eingesetzt werden.

1. Welche Einsätze von IT-Kräften der Bundeswehr, insbesondere der CNO-Einheit sowie deren Nachfolgeinstitutionen, wie dem Zentrum Cyber-Operationen, gab es seit Gründung der CNO (Computer-Netzwerk-Operationen) im Jahr 2006?

Der Einsatz von IT-Fähigkeiten, u. a. zur Sicherstellung der Führungsfähigkeit, ist inhärenter Bestandteil jeglicher Einsatzplanung und -führung.

Für die weitere Beantwortung der Frage 1 wird auf den als „VS – Nur für den Dienstgebrauch“* eingestuften Antwortteil verwiesen. Der parlamentarische Informationsanspruch ist zwar grundsätzlich für die Beantwortung gestellter Fragen in der Öffentlichkeit ausgelegt, die Bundesregierung ist allerdings nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 1 nicht vollständig in offener Form erfolgen kann. Die Einstufung der Antwort zu Frage 1 als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“* wird im Hinblick auf das Staatswohl als erforderlich erachtet, da die in der Antwort aufgeführten Fähigkeiten unter Umständen Rückschlüsse auf den in den aufgeführten Einsätzen zur Verfügung stehenden Fähigkeitsumfang zulassen. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen des Bundesministeriums des Innern, für Bau und Heimat (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Im vorliegenden Fall werden diese Informationen daher als „VS – Nur für den Dienstgebrauch“* eingestuft und dem Deutschen Bundestag gesondert übermittelt.

2. Welche Kräfte innerhalb des Kommando CIR (Cyber- und Informationsraum) sind für die kontinuierliche Lagebildaufklärung im „Cyber-Raum“ zuständig?

Ein Auftrag des Kommando Cyber- und Informationsraum (KdoCIR) ist die Erstellung eines umfassenden Lagebildes des Cyber- und Informationsraumes. Dazu leisten alle ihm unterstellten Kräfte einen Beitrag.

3. Welche anderen Bereiche bzw. Einheiten der Bundeswehr sowie externer Stellen wie beispielsweise der Nachrichtendienste sind an der Lagebildaufklärung im „Cyber-Raum“ beteiligt, und in welchem Umfang?

Zum Lagebild des Cyber- und Informationsraumes können alle Bereiche/Einheiten der Bundeswehr anlassbezogen beitragen.

Im Nationalen Cyber-Abwehrzentrum tauschen die für Cyber-Sicherheitsfragen zuständigen Bundesbehörden Informationen zu Cyber-Vorfällen aus. Im Nationalen Cyber-Abwehrzentrum sind das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Bevölkerungsschutz und Katastrophen-

---

* Das Bundesministerium der Verteidigung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

hilfe (BBK), das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), das Bundespolizeipräsidium (BPOL), das Zollkriminalamt (ZKA) und die Bundeswehr durch das KdoCIR sowie das Bundesamt für den Militärischen Abschirmdienst (BAMAD) vertreten.

4. Inwieweit werden im Rahmen der Vorfeldaufklärung in Friedenszeiten bzw. außerhalb nur im bewaffneten Konflikt geltender spezifischer Befugnisse auch fremde IT-Systeme analysiert?

Die erfragten Informationen zielen im Kern auf die Offenlegung von Erkenntnisinteressen der Bundesregierung sowie bestimmter Arbeitsmethoden und Vorgehensweisen im Bereich der technischen Aufklärung. Solche Informationen sind im Hinblick auf die künftige Erfüllung des verfassungsgemäßen Auftrages der Streitkräfte jedoch besonders schutzwürdig, der Schutz der technischen Aufklärungsfähigkeiten stellt für die Aufgabenerfüllung einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität der Aufklärung durch den Einsatz spezifischer technischer Fähigkeiten und damit dem Staatswohl. Das Bekanntwerden der näheren Umstände der technischen Aufklärungsfähigkeiten, -tätigkeiten und Analysemethoden sowie der Erkenntnisinteressen könnte das Wohl des Bundes gefährden. Eine (zur Veröffentlichung bestimmte) Antwort der Bundesregierung (auf diese Frage) würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass auch bestehende oder in der Entwicklung befindliche Fähigkeiten und Methoden aufgeklärt und damit der Einsatzerfolg gefährdet würde. Es könnten entsprechende Abwehrstrategien entwickelt werden. Dies könnte einen Nachteil für die wirksame Aufgabenerfüllung der Sicherheitsbehörden sowie der Streitkräfte und damit für die Interessen der Bundesrepublik Deutschland bedeuten.

Die Fragestellung berührt derart schutzbedürftige Geheimhaltungsinteressen, dass auch ein geringfügiges Risiko des Bekanntwerdens, wie es auch bei einer Übermittlung an die Geheimschutzstelle des Deutschen Bundestages nicht ausgeschlossen werden kann, aus Staatswohlgründen vermieden werden muss. In diesem Fall überwiegt daher das Staatswohlinteresse gegenüber dem parlamentarischen Informationsrecht.

5. Wodurch wird dabei der völkerrechtlich gebotenen Differenzierung zwischen staatlichen und privaten Akteuren bzw. IT-Systemen Rechnung getragen?

Der Einsatz von Cyber-Fähigkeiten der Bundeswehr muss sich stets im Rahmen des geltenden Völkerrechts bewegen. Soweit dazu Differenzierungen in Hinblick auf den völkerrechtlichen Status des Ziels einer Maßnahme erforderlich sein sollten, ist und wird dem durch entsprechende Vorkehrungen auf allen Ebenen Rechnung getragen.

6. Welche Kooperationen von IT-Kräften der Bundeswehr, des Kommando CIR, der CNO-Einheit sowie deren Nachfolgeinstitutionen wie dem Zentrum Cyber-Operationen mit anderen deutschen staatlichen Stellen bzw. Nachrichtendiensten gab und gibt es?

   In welchen Anteilen wurden und werden hier welche Aufgaben erfüllt, und zu welchen Zwecken?

Zwischen KdoCIR und BAMAD besteht eine Kooperationsvereinbarung zum Austausch von Informationen im Rahmen der gesetzlichen Bestimmungen. KdoCIR und das BAMAD tauschen insbesondere im Nationalen Cyber-Abwehrzentrum mit anderen Behörden Informationen zu Cyber-Vorfällen aus. Auf die Antwort zu Frage 3 wird verwiesen. Darüber hinaus gehende Aktivitäten finden im Rahmen der jeweiligen verfassungsrechtlichen bzw. gesetzlichen Aufgabenerfüllung statt.

7. Inwieweit wurden und werden durch IT-Kräfte der Bundeswehr, das Kommando CIR, die CNO-Einheit sowie deren Nachfolgeinstitutionen wie das Zentrum Cyber-Operationen oder andere Stellen im Geschäftsbereich des Bundesministeriums der Verteidigung Exploits bzw. Schwachstellen in IT-Produkten (Soft- und Hardware) mit dem Ziel der Ausnutzung dieser Schwachstellen für Aufklärung oder offensives Wirken im „Cyber-Raum“

   a) eigenständig gesucht,

   b) angekauft (bitte unter nachvollziehbarer, präziser Angabe der zugrunde gelegten Haushaltstitel auflisten) bzw.

   c) durch Kooperationen mit anderen Diensten oder Staaten bereitgestellt?

Die erfragten Informationen zielen im Kern auf die Offenlegung bestimmter Arbeitsmethoden und Vorgehensweisen im Bereich militärischer Cyber-Operationen. Solche Arbeitsmethoden sind im Hinblick auf die künftige Erfüllung des verfassungsgemäßen Auftrages der Streitkräfte jedoch besonders schutzwürdig, der Schutz insbesondere der technischen Aufklärungsfähigkeiten stellt für die Aufgabenerfüllung der Streitkräfte einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität der Aufklärung durch den Einsatz spezifisch technischer Fähigkeiten und damit dem Staatswohl. Das Bekanntwerden der näheren Umstände der technischen Aufklärungsfähigkeiten, -tätigkeiten und Analysemethoden könnte das Wohl des Bundes gefährden. Eine (zur Veröffentlichung bestimmte) Antwort der Bundesregierung (auf diese Frage) würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass auch bestehende oder in der Entwicklung befindliche Fähigkeiten und Methoden aufgeklärt und damit der Einsatzerfolg gefährdet würde. Es könnten entsprechende Abwehrstrategien entwickelt werden. Dies könnte einen Nachteil für die wirksame Aufgabenerfüllung der Streitkräfte und damit für die Interessen der Bundesrepublik Deutschland bedeuten.

Die Fragestellung berührt derart schutzbedürftige Geheimhaltungsinteressen, dass auch ein geringfügiges Risiko des Bekanntwerdens, wie es auch bei einer Übermittlung an die Geheimschutzstelle des Deutschen Bundestages nicht ausgeschlossen werden kann, aus Staatswohlgründen vermieden werden muss. In diesem Fall überwiegt daher das Staatswohlinteresse gegenüber dem parlamentarischen Informationsrecht.

8. Inwieweit existiert derzeit eine Praxis im Geschäftsbereich des Bundesverteidigungsministeriums und nachgeordneter Stellen, erkannte Schwachstellen in IT-Produkten (Soft- und Hardware) zu melden bzw. veröffentlichen?

Die durch die Informationssicherheitsorganisation der Bundeswehr in den eigenen Systemen identifizierten Sicherheitslücken werden an den jeweils zuständigen Informationssicherheitsbeauftragten des/der betroffenen Projekte und der betroffenen Dienststelle/-n zur Abstellung gemeldet. Entdeckte Sicherheitslücken werden gemäß § 4 des BSI-Gesetzes ebenfalls an das Bundesamt für Sicherheit in der Informationstechnik gemeldet.

9. Inwieweit und unter welchen Bedingungen werden Sicherheitslücken – sofern sie verwendet werden – zurückgehalten für eine spätere Nutzung?

   Inwiefern findet ein kontinuierlicher Prozess der Abwägung über deren Veröffentlichung statt (im Sinne eines Vulnerabilities Equities Process)?

Die Ausgestaltung eines Prozesses zum verantwortungsvollen Schwachstellenmanagement im Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) wird derzeit untersucht. Die Untersuchungen sind noch nicht abgeschlossen.

10. Welche Ansätze im Zuständigkeitsbereich der gesamten Bundesregierung gibt es, im Interesse der IT-Sicherheit darauf hinzuwirken, dass

    a) ausnahmslos alle bekannt werdenden Sicherheitslücken gemeldet und geschlossen werden und nicht zur Infiltration von Netzen genutzt werden dürfen, und

    b) an diese Verpflichtungen auch staatliche Stellen – einschließlich Geheimdiensten und Stellen im Geschäftsbereich des Bundesverteidigungsministeriums und nachgeordneter Behörden – gebunden werden, d. h. die Meldepflichten auch für diese gelten und ihnen die Nutzung von Exploits bzw. Schwachstellen untersagt wird?

Die Fragen 10 bis 10b werden aufgrund ihres inhaltlichen Zusammenhanges gemeinsam beantwortet.

Die Ausgestaltung eines Prozesses zum verantwortungsvollen Schwachstellenmanagement der Bundesregierung wird derzeit intensiv erörtert. Die Überlegungen sind noch nicht abgeschlossen.

11. Welche Kooperationen oder Bedarfsmeldungen gibt es seitens des Kommando CIR an die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) sowie an die neue Agentur für Innovation in der Cybersicherheit?

Konkrete Kooperationsvereinbarungen oder Bedarfsmeldungen im Sinne der Fragestellung existieren derzeit nicht.

12. Welche Einsatzszenarien wurden und werden durch die CNO-Einheit sowie deren Nachfolgeinstitutionen wie das Zentrum Cyber-Operationen geübt?

    Für welche strategischen Aufgaben und Ziele planen diese IT-Kräfte?

Die Einsatzszenarien, Aufgaben und Ziele des Zentrum Cyber-Operationen (ZCO) leiten sich aus denen der Bundeswehr ab und decken damit das internationale Krisenmanagement, die Landes- und Bündnisverteidigung, die Beiträge zu Heimatschutz sowie nationaler Krisen- und Risikovorsorge und subsidiäre Unterstützungsleistungen ab.

13. Welche Einheiten im Geschäftsbereich des Bundesverteidigungsministeriums außer der CNO-Einheit sowie deren Nachfolgeinstitution Zentrum Cyber-Operationen verfügen über Fähigkeiten zum „Wirken im Cyber-Raum“?

Im Geschäftsbereich BMVg verfügen keine weiteren Einheiten über die Fähigkeiten im Sinne der Fragestellung.

14. In welchem quantitativen und qualitativen Verhältnis steht bei der Aus- oder Fortbildung von IT-Kräften, im Kommando CIR, bei der CNO-Einheit sowie deren Nachfolgeinstitutionen wie dem Zentrum Cyber-Operationen der Bundeswehr das Vermitteln offensiver Fähigkeiten und Fähigkeiten zum „Wirken in fremden Netzen“ zum Erwerb und der Vermittlung von Fähigkeiten zur Härtung von IT-Systemen?

Die „IT-Kräfte“ sind hinsichtlich ihrer Kernaufträge und den dafür notwendigen Fähigkeiten und Fertigkeiten zu unterscheiden. Daher unterscheiden sich auch die jeweiligen Ausbildungsgänge hinsichtlich ihrer Inhalte.

Das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) hat den Auftrag, den Schutz und sicheren Betrieb der IT-Systeme der Bundeswehr zu gewährleisten.

Entsprechend richten sich alle Aus-, Fort- und Weiterbildungsmaßnahmen an der Fähigkeit zur Härtung von IT-Systemen aus. Diese umfassen Trainings zur Basisausbildung an Bildungseinrichtungen der Bundeswehr sowie Trainings zur Qualifizierung bei der Industrie oder durch Inhouse-Schulungen.

Das Zentrum Cyber-Operationen (ZCO) ist das Kernelement der Bundeswehr für Aufklärung und Wirkung im Sinne der Fragestellung. Die Aus-, Fort- und Weiterbildung orientiert sich an diesem Ziel und erfolgt ausschließlich für Personal des ZCO.

15. Inwieweit und konkret durch welche Verfahrensschritte wird bei der Auswahl von Bewerberinnen und Bewerbern, der Nachqualifikation von Mannschaften und der Ausbildung aller (zukünftigen) IT-Kräfte im Geschäftsbereich des Bundesverteidigungsministeriums darauf geachtet und sichergestellt, dass diese qualifiziertes Fachwissen über Stabilität, Sicherheit, Zuverlässigkeit von IT-Systemen und auch darüber besitzen bzw. erwerben, wie typische Angriffe auf die IT-Infrastruktur funktionieren und wie Hard- und Software schon bei der Entwicklung dagegen geschützt werden kann?

Im Rahmen der Erstellung von Ausschreibungen bzw. Dienstpostenbeschreibungen werden erforderliche Qualifikationsmerkmale aufgenommen. Die Feststellung des tatsächlichen Fachwissens erfolgt im Rahmen von Interviews und Tests, darauf basierend erfolgt eine ggf. notwendige Weiterqualifizierung im Rahmen

der Bildungseinrichtungen der Bundeswehr, durch Inhouse-Ausbildung/Ausbildung am Arbeitsplatz sowie durch Lehrgänge und Zertifizierungen der freien Wirtschaft.

Im Zuge der Aus-, Fort- und Weiterbildung werden Aspekte der Cybersicherheit berücksichtigt. Eine spezifische Ausbildung zum Schutz eigener Systeme erfolgt insbesondere für Personal des ZCSBw und weiteres IT-Fachpersonal mit Schwerpunktätigkeit in der IT-Sicherheit.

16. Welche Planungen – sowohl personell als auch hinsichtlich technischer Fähigkeiten – gibt es im Kommando CIR über 2021 hinaus?

Im KdoCIR wird damit geplant, dass der OrgBerCIR im Jahr 2021 die Zielstruktur im Rahmen der ausplanbaren Dienstpostenumfänge einnimmt. Die personellen und materiellen Strukturen werden dabei kontinuierlich auftrags- und fähigkeitsorientiert auf Notwendigkeit, Zweckmäßigkeit und Wirtschaftlichkeit überprüft und bei Bedarf unter Anwendung gültiger, anerkannter Verfahren angepasst.

Hinsichtlich der technischen Fähigkeiten wurden die vorrangigsten Ziele im Cyber- und Informationsraum wie folgt gesetzt:

- Auf- und Ausbau von Fähigkeiten zur Cyber-Verteidigung zum Erhalt der sicheren Nutzung des Cyber-Raums Deutschlands als Dauereinsatzaufgabe.
- Auf- und Ausbau eines Gemeinsamen Lagezentrums zur Sicherstellung eines umfassenden Lagebildes Cyber- und Informationsraum für den Geschäftsbereich BMVg und als Grundlage der Operationsführung in der Dimension CIR (inkl. Planung, Durchführung und Überwachung).
- Erhalt und Ausbau der Teilhabe am Nationalen Cyber-Abwehrzentrum und Erstellung Echtzeit-Lagebild Cyber Bundeswehr für den ressortübergreifenden Informationsaustausch.

17. Inwieweit ist beabsichtigt, das Parlament über die offensiven Fähigkeiten bzw. Fähigkeiten zum „Wirken im Cyber-Raum“ zu unterrichten, die erworben werden durch IT-Kräfte der Bundeswehr, das Kommando CIR, die CNO-Einheit sowie deren Nachfolgeinstitutionen wie das Zentrum Cyber-Operationen oder andere Stellen im Geschäftsbereich des Bundesverteidigungsministeriums?

In welcher Form und in welchem Detailumfang?

Die Bundeswehr unterliegt einer umfassenden, verfassungsrechtlich vorgegebenen parlamentarischen Kontrolle. Dies umfasst auch militärische Fähigkeiten und Maßnahmen im Cyber- und Informationsraum. Es gelten die gleichen Informations- und Kontrollrechte wie für sonstige Maßnahmen der Streitkräfte. Das Parlament wird darüber hinaus zweimal jährlich im Rahmen des „Berichtes des BMVg für Rüstungsangelegenheiten“ detailliert über die wesentlichen Rüstungsprojekte informiert. Weiterhin erstellt das BMVg auf Antrag des Haushaltsausschusses des Deutschen Bundestages seit 2018 den Sachstandsbericht „Cyber- und Informationsraum“.

18. In welcher Form konkret ist eine Beteiligung des Parlaments vor dem Einsatz offensiver Fähigkeiten bzw. Fähigkeiten zum „Wirken im Cyber-Raum“ durch IT-Kräfte der Bundeswehr, das Kommando CIR, die CNO-Einheit sowie deren Nachfolgeinstitutionen wie das Zentrum Cyber-Operationen oder andere Stellen im Geschäftsbereich des Bundesverteidigungsministeriums realisiert oder beabsichtigt?

Militärische Maßnahmen im Cyberraum unterliegen dem gleichen rechtlichen Rahmen wie andere militärische Maßnahmen auch und können entsprechend durchgeführt werden. Soweit erforderlich findet dabei die Beteiligung des Parlamentes gemäß dem Parlamentsbeteiligungsgesetz statt.

Ergänzend wird auf die Antwort der Bundesregierung zu den Fragen 1 bis 3 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/5472 verwiesen.

19. Welche Fähigkeiten aus dem IT-Bereich sollen der NATO zur Verfügung gestellt werden (vgl. www.zeit.de/news/2019-02/14/deutschland-stellt-nato-mittel-fuer-militaerische-cyber-einsaetze-zur-verfuegung-20181004-doc-19r778)?

Gegenüber der NATO wurde die grundsätzliche Bereitschaft angezeigt, zukünftig die Erzielung militärischer Effekte im Rahmen von NATO-geführten Operationen auch mit Cyber-Operationen als nationalem, souveränen Beitrag zu unterstützen. Der Einsatz von Cyberfähigkeiten erfolgt anlassbezogen im konkreten Einzelfall und nach souveräner Entscheidung, unter Beibehaltung nationaler politischer und rechtlicher Vorbehalte.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333